The Examiner failed to note that the same reference does, however, go on in the next sentence to note that such a search would be "of value *only if it were computationally feasible*" (emphasis added). In other words, although theoretically the seed can be obtained, in practice there are pseudorandom sequences for which the seed cannot be practically obtained. The section cited by the Examiner develops this theme, noting that certain generators are predictable and the development of general notions that emerge in subsequent sections include unpredictable pseudorandom generators. Given that a pseudorandom generator is deterministic as established by the passage relied on by the Examiner, the reference relied upon by the Examiner lends support for Applicants' use of the terminology" deterministic but unpredictable manner." In other words, this reference itself clearly suggests the existence of a device that operates in an **"unpredictable but deterministic manner."**

The text "Applied Cryptography" by Bruce Schneier (ISBN 0-471-59756-2), at pages 39 through 41, discusses pseudorandom sequence generation i.e. in a deterministic manner and the concept of unpredictability. A copy of this section, together with face page of the book, is attached. From this section it would be noted that pseudorandom generators are deterministic in nature but within the general class of pseudorandom generation there are sub-classes that are suitable for cryptographic applications. A condition for a cryptographically random sequence is not only that it looks random but it must have the additional second property, namely, that it is *unpredictable.* The term "unpredictable" as applied in this art means "it must be computationally unfeasible to predict what the next random bit will be, given complete knowledge of the algorithms or hardware generating the sequence and all of the previous bits in the stream." Thus it may be seen that pseudorandom generators are deterministic, but they are also unpredictable if they satisfy the above requirement.

Quite clearly therefore within the context of cryptography there is a well established concept of operating in a deterministic but unpredictable manner and this is readily understood by those skilled in the particular art to which the present invention pertains.

The use of this concept is not restricted to the Schneier publication. Attached is an extract from a further publication by Kranakis namely "Theoretical Aspects of the Security of Public Key Cryptography" in which, at page 105, he makes reference to two security tests for

pseudorandom generators. The first one, the Blum-Mical test, is used to construct unpredictable pseudorandom generators. In other words, he is using terminology of a generator that operates in an unpredictable and pseudorandom or deterministic manner. Also enclosed is an extract from "Pseudorandomness and Crytographic Applications" by Michael Luby. At page 51, at Theorem 4.1, he defines a pseudorandom (deterministic) generator if and only if the generator is "next-bit unpredictable." Again the concepts of a deterministic operation with unpredictability are used.

It is submitted therefore that independent claims 13 and 21 to satisfy the requirements of 35 U.S.C. 112, second paragraph, in that they utilize language which is readily understood by a person skilled in the art to which the present invention pertains. The widespread use of that language has been demonstrated from a number of sources including the source relied upon by the Examiner and is therefore believed to provide a clear showing that the language of claims 13 and 21 is allowable. Further consideration to that end is respectfully requested. Claims 14-20 and 22-27 depend from and serve to further limit and define the invention of the independent claims.

Respectfully submitted,

11/5/99
Date

Lawrence A. Maxham
Attorney for the Applicant
Registration No. 24,483